IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Before the Board of Patent Appeals and Interferences

Appellants:	Junbiao Zhang et al.
Serial No.:	10/549,408
Filed:	September 14, 2005
For:	WLAN SESSION MANAGEMENT TECHNIQUES WITH SECURE REKEYING AND LOGOFF
Examiner:	Syed Zia
Art Unit:	2431
Conf. No.:	1829

Mail Stop APPEAL BRIEF
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia, 22313-1450

CORRECTED APPEAL BRIEF

May it please the Honorable Board:

In response to the Notification by the Examiner dated 22 September 2009, the Appellants hereby submit this Corrected Brief on Appeal from the rejection of Claims 1 to 24. The fee for filing this Brief has been previously paid. The Appellants waive an Oral Hearing for this appeal.

Please charge any additional fee or credit any overpayment to Deposit Account No. 07-0832. Enclosed is a single copy of this Brief

I. REAL PARTY IN INTERST

The real party in interest of Application Serial No.10/549408 is the Assignee of record:

Thomson Licensing

46, Quai A. Le Gallo

F-92100 Boulogne-Billancourt

FRANCE

II. RELATED APPEALS AND INTERFERENCES

There are currently, and have been, no related interferences regarding Application Serial No. 10/549,408, known to the undersigned attorney. The Appellants have previously filed an appeal from the Examiners' rejection dated 7 August 2008; however, that rejection was withdrawn, and prosecution has been reopened.

III. STATUS OF THE CLAIMS

Claims 1 to 24 are rejected, and the rejection of Claims 1 to 24 is appealed.

IV. STATUS OF AMENDMENTS

All amendments were entered and are reflected in the Claims listed in Appendix I.

V. SUMMARY OF CLAIMED SUBJECT MATTER

Independent Claim 1 claims a method for providing a secure communications session with a user terminal in a communications network, the method comprising the steps of:

transmitting a secure key and a secure seed (page 3, lines 9-11) to the user terminal using a secure communications method, the secure key and the secure

seed being suitable for storage in the user terminal (page 3, lines 8-10) for use during the secure communications session;

encrypting and transmitting data to the user terminal using a current session key (page 4, lines 6-9), and receiving and decrypting data received from the user terminal using the current session key, the secure key initially being used as the current session key (page 4, lines 9-10); and

periodically generating by an access point a subsequent session key using the secure seed and using the subsequent session key as the current session key during subsequent communications between the communications network and the user terminal (page 4, lines 10-12).

Independent Claim 4 claims a method for providing a secure communications session with a mobile terminal in a wireless local area network, the method comprising the steps of:

transmitting a secure key and a secure seed to the mobile terminal using a secure communications method (page 3, lines 9-11), the secure key and the secure seed being suitable for storage in the mobile terminal for use during the secure communications session (page 3, lines 8-10);

encrypting and transmitting data to the mobile terminal using a current session key, and receiving and decrypting data received from the mobile terminal using the current session key (page 4, lines 6-9), the secure key initially being used as the current session key (page 4, lines 9-10); and

periodically generating by an access point a subsequent session key using the secure seed and using the subsequent session key as the current session key during subsequent communications with the mobile terminal (page 4, lines 10-12).

Independent Claim 7 claims a method for providing a secure communications session with a mobile terminal in a wireless local area network, the method comprising the steps of:

generating a secure key (page 4, line 4);

transmitting the secure key to the mobile terminal using a secure communications method, the secure key being stored in the mobile terminal for use during the secure communications session (page 4, lines 5-7);

encrypting and transmitting data to the mobile terminal using a current session key, and receiving and decrypting data received from the mobile terminal using the current session key (page 4, lines 7-9); and

ending the secure communications session by an access point in response to receiving a logoff message from the mobile terminal, the logoff message being in encrypted form and including the secure key (page 3, lines 27-29).

Independent Claim 8 claims a method for providing a secure communications session with a mobile terminal in a wireless local area network, the method comprising the steps of:

generating a secure key and a secure seed (page 4, lines 3-10);

transmitting the secure key and the secure seed to the wireless local area network using a secure communications method, the secure key and the secure seed being stored in the wireless local area network for use during the secure communications session (page 3, lines 1-4);

encrypting and transmitting data to the wireless local area network using a current session key, and receiving and decrypting data received from the wireless local area network using the current session key, the secure key initially being used as the current session key (page 4, lines 7-10); and

periodically generating by the mobile terminal a subsequent session key using the secure seed and using the subsequent session key as the current session key during subsequent communications with the wireless local area network (page 4, lines 10-12).

Independent Claim 11 claims a method for providing a secure communications session with a mobile terminal in a wireless local area network, the method comprising the steps of:

generating a secure key (page 4, line 3);

receiving the secure key from the wireless local area network using a secure communications method, the secure key being stored in the wireless local area network for use during the secure communications session (page 3, lines 9-11);

encrypting and transmitting data to the wireless local area network using a current session key, and receiving and decrypting data received from the wireless local area network using the current session key (page 4, lines 6-9); and

ending the secure communications session in response to receiving a logoff message from the wireless local area network, the logoff message being in encrypted form and including the secure key (page 3, lines 15-23).

Independent Claim 12 claims a method for providing a secure communications session with a mobile terminal in a wireless local area network, the method comprising the steps of:

installing at least two shared secrets on both the mobile terminal and the wireless local area network access point during the user authentication phase whereby a first secret is the initial session key and a second secret is utilized as secure seed to generate subsequent session keys (page 3, lines 6-12).

Independent Claim 18 claims a method for providing a secure communications session between a mobile terminal and a wireless local area network, the method comprising the steps of:

a mobile terminal sending during session logoff an encrypted logoff request accompanied by the secure seed such that the secure seed appears in the logoff request (page 3, lines 28-31).

Independent Claim 19 claims an access point for providing a secure communications session between a mobile terminal and a wireless local area network, comprising:

a means for transmitting a secure key and a secure seed to the mobile terminal using a secure communications method (page 4, lines 18-20);

a means to encrypt data using the secure key (page 4, lines 20-21); and

a means to periodically generate a subsequent session key using the secure seed (page 4, lines 20-22; page 5, lines 11-16).

Independent Claim 20 claims a terminal device for providing a secure communications session with a communications network, comprising:

a means to receive a secure key and a secure seed and a means to store the secure key and the secure seed for use during the secure communications session (page 3, lines 9-10);

a means to receive data and a means to decrypt the data using a current session key during the secure communications session, the secure key being using initially as the current session key (page 4, lines 8-10); and

a means to generate a subsequent session key using the current session key and the secure seed, the subsequent session key thereafter being used as the current session key for subsequent communications (page 9, lines 7-19; page 5, lines 11-16).

Independent Claim 24 claims an access point (130_n) for providing a secure communications session between a mobile terminal and a wireless local area network, comprising:

a means (420) to transmit a secure key and a secure seed and a means to store the secure key and the secure seed for use during the secure communications session;

a means (415) to encrypt data and a means to transmit data to the mobile terminal and a means to receive data and a means (435) to decrypt the data from the mobile terminal using a current session key during the secure communications session, the secure key being using initially as the current session key (page 9, lines 14-16); and

a means (425) to generate a subsequent session key using the current session key and the secure seed, the subsequent session key thereafter being used as the current session key for subsequent communications (page 9, lines 17-19).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The Examiner has rejected Claims 1-24 under 35 USC 102(e) as being anticipated by US 2006/0022085 to Ferman.

VII. ARGUMENT

This invention relates to a security arrangement for communication between a user and a network. Nowhere does the cited reference relate to a security arrangement for communication between a user and a network. Rather, US 2006/0022085 to Ferman relates to control of wing and stabilizer surfaces in an aircraft. Perhaps the Examiner meant to rely upon US 2006/0052085 to Gregrio Rodriguez et al., which is one of the nine (9) U.S. Patent Documents listed on PTO-892, but not relied upon in the Examiner's rejection. In order to expedite this appeal, the Appellants will assume that the Examiner intended to rely upon US 2006/0052085 to Gregrio Rodriguez et al.

Nowhere do Gregrio Rodriguez et al show or suggest the instant invention. More specifically, nowhere do Gregrio Rodriguez et al show or suggest:

> "periodically generating by an access point a subsequent session key using the secure seed and using the subsequent session key as the current session key during subsequent communications between the communications network and the user terminal",

as specifically recited in Claim 1. Rather, Gregrio Rodriguez et al use the same session key (AKA encryption key Kc) for subsequent communications. Nowhere do Gregrio Rodriguez et al periodically generate a subsequent session key. See ¶0065 of Gregrio Rodriguez et al.

The Examiner has asserted that Gregrio Rodriguez et al show periodically generating by an access point a subsequent session key using the second secure key and using the subsequent session key as the current session key during subsequent communications between the communications network and the user terminal. The Appellants can not agree. Nowhere do Gregrio Rodriguez et al. show or suggest this step of the inventive method. It is therefore clear that Gregrio Rodriguez et al do not affect the patentability of Claim 1.

Similarly nowhere do Gregrio Rodriguez et al show or suggest:

"periodically generating by an access point a subsequent session key using the secure seed and using the subsequent session key as the current session key during subsequent communications with the mobile terminal.",

as specifically recited in Claim 4. Rather, Gregrio Rodriguez et al use the same session key for subsequent communications. Nowhere do Gregrio Rodriguez et al periodically generate a subsequent session key, as explained above.

The Examiner has asserted that Gregrio Rodriguez et al. teach and describe periodically generating a subsequent session key using the second secure key and using the subsequent session key as the current session key during subsequent communications with the mobile terminal. The Appellants can not agree. Nowhere do Gregrio Rodriguez et al show or suggest this step of the inventive method. It is therefore clear that Gregrio Rodriguez et al do not affect the patentability of Claim 4.

Similarly, nowhere do Gregrio Rodriguez et al show or suggest:

"ending the secure communications session by an access point in response to receiving a logoff message from the mobile terminal, the logoff message being in encrypted form and including the secure key.",

as specifically recited in Claim 7. Nowhere do Gregrio Rodriguez et al disclose a logoff message in encrypted form and including the secure key.

The Examiner has asserted that Gregrio Rodriguez et al. teach and describe ending the secure communication session by an access point in response to receiving a logoff message from the mobile terminal, the logoff message being in an encrypted form and including the secure key. The Appellants can not agree. Nowhere do Gregrio Rodriguez et al teach or suggest this step of the inventive method. The Appellants therefore submit that the patentability of Claim 7 is not affected by Gregrio Rodriguez et al.

Similarly, nowhere do Gregrio Rodriguez et al show or suggest:

"periodically generating by the mobile terminal a subsequent session key using the secure seed and using the subsequent session key as the current session key during subsequent communications with the wireless local area network.",

as specifically recited in Claim 8. Nowhere do Gregrio Rodriguez et al periodically generate a subsequent session key.

The Examiner has asserted that Gregrio Rodriguez et al. teach and describe periodically generating by the mobile terminal a subsequent session key using the second secure key and using the subsequent session key as the current session key during subsequent communications with the wireless local area network. The Appellants can not agree. Nowhere do Gregrio Rodriguez et al teach or suggest this step of the method. The Appellants therefore submit that Gregrio Rodriguez et al does not affect the patentability of Claim 8.

Similarly nowhere do Gregrio Rodriguez et al show or suggest:

"ending the secure communication session in response to receiving a logoff message from the wireless local area network, the logoff message being in encrypted form and including the secure key.",

as specifically set forth in Claim 11. Nowhere do Gregrio Rodriguez et al disclose a logoff message being in encrypted form and including the secure key.

The Examiner has asserted that Gregrio Rodriguez et al. teach and describe ending the secure communication session in response to receiving a logoff message from the WLAN, the logoff message being in encrypted form and including the secure key. The Appellants can not agree. Nowhere do Gregrio Rodriguez et al show or suggest this step of the method. It is therefore clear that Gregrio Rodriguez et al do not affect the patentability of the invention set forth in Claim 11.

Similarly nowhere do Gregrio Rodriguez et al teach or suggest:

"a second secret is utilized as secure seed to generate subsequent session keys",

as specifically recited in Claim 12. Nowhere do Gregrio Rodriguez et al. generate subsequent session keys. Rather, Gregrio Rodriguez et al. use only one session key.

The Examiner has asserted that Gregrio Rodriguez et al. teach and describe a second secret utilized as secure seed to generate subsequent session keys. The Appellants can not agree. Nowhere do Gregrio Rodriguez et al. show or suggest this step of the method. It is therefore clear that the patentability of the invention as defined by Claim 12 is not affected by Gregrio Rodriguez et al.

Similarly, nowhere does Gregrio Rodriguez et al show or suggest:

"a mobile terminal sending during session logoff an encrypted logoff request accompanied by the secure seed such that the secure seed appears in the logoff request.",

as specifically recited in Claim 18. Nowhere do Gregrio Rodriguez et al. send an encrypted logoff request accompanied by the secure seed The Examiner has asserted that Gregrio Rodriguez et al teach and describe a mobile terminal sending during session logoff an encrypted logoff request accompanied by the secure seed such that the secure seed appears in the logoff request. The Appellants can not agree. Nowhere do Gregrio Rodriguez et al. teach or suggest this step of the method. It is therefore clear that the patentability of the invention as defined by Claim 18 is not affected by Gregrio Rodriguez et al.

Similarly nowhere do Gregrio Rodriguez et al show or suggest:

"a means to periodically generate a subsequent session key using the secure seed.",

as specifically set forth in Claim 19. Nowhere do Gregrio Rodriguez et al periodically generate a subsequent session key.

The Examiner has asserted that Gregrio Rodriguez et al. teach and describe a means to periodically generate a subsequent session key using the second secure

key. The Appellants can not agree. Nowhere do Gregrio Rodriguez et al. teach or suggest this structure. It is therefore clear that Gregrio Rodriguez et al. does not affect the patentability of the invention defined by Claim 19.

Similarly, nowhere do Gregrio Rodriguez et al show or suggest:

"a means to generate a subsequent session key using the current session key and the secure seed, the subsequent session key thereafter being used as the current session key for subsequent communications.",

as specifically set forth in Claim 20. Rather, nowhere do Gregrio Rodriguez et al teach or suggest a means to generate a subsequent session key. Rather, Gregrio Rodriguez et al. use the same session key.

The Examiner has asserted that Gregrio Rodriguez et al. teach and describe a means to generate a subsequent session key using the current session key and the secure seed, the subsequent session key thereafter being used as a current session key for subsequent communications. The Appellants can not agree. Nowhere do Gregrio Rodriguez et al teach or suggest this structure. It is therefore clear that Gregrio Rodriguez et al do not affect the patentability of Claim 20.

Similarly, nowhere do Gregrio Rodriguez et al show or suggest:

"the means to generate a subsequent session key using the current session key and the secure seed, the subsequent session key thereafter being used as the current session key for subsequent communications.",

as specifically set forth in Claim 24. Nowhere do Gregrio Rodriguez et al. generate a subsequent session key.

The Examiner has asserted that Gregrio Rodriguez et al. teach and describe a means to generate a subsequent session key using the current session key and the secure seed, the subsequent session key thereafter being used as the current session key for subsequent communications. The Appellants can not agree. Nowhere do Gregrio Rodriguez et al. teach or suggest this structure. It is therefore clear that Gregrio Rodriguez et al do not affect the patentability of Claim 24.

Claims 2 and 3 are dependent from Claim 1, and add further advantageous features. The Appellants submit that these subclaims are patentable as their parent Claim 1.

Claims 5 and 6 are dependent from Claim 4, and add further advantageous features. The Appellants submit that these subclaims are patentable as their parent Claim 4.

Claims 9 and 10 are dependent from Claim 8 and add further advantageous features. The Appellants submit that these subclaims are patentable as their parent Claim 8.

Claims 13 to 17 are dependent from Claim 12 and add further advantageous features. The Appellants submit that these subclaims are patentable as their parent Claim 12.

Claim 21 is dependent from Claim 20 and adds further advantageous features. The Appellants submit that this subclaim is patentable as its parent Claim 20.

Claims 22 and 23 are dependent from Claim 24 and add further advantageous features. The Appellants submit that these subclaims are patentable as their parent Claim 24.

The Appellants submit that all of the Claims are allowable, and that the Rejection should be reversed.

Respectfully submitted,
JUNBIAO ZHANG ET AL.

By: /Daniel E. Sragow/
Daniel E. Sragow, Attorney
Reg. No. 22,856
(609) 734-6832

DES:pdf

Patent Operations
Thomson Licensing LLC
P.O. Box 5312
Princeton, NJ 08543-5312
2 October 2009

APPENDIX I. APPEALED CLAIMS

1. A method for providing a secure communications session with a user terminal in a communications network, the method comprising the steps of:

transmitting a secure key and a secure seed to the user terminal using a secure communications method, the secure key and the secure seed being suitable for storage in the user terminal for use during the secure communications session;

encrypting and transmitting data to the user terminal using a current session key, and receiving and decrypting data received from the user terminal using the current session key, the secure key initially being used as the current session key; and

periodically generating by an access point a subsequent session key using the secure seed and using the subsequent session key as the current session key during subsequent communications between the communications network and the user terminal.

2. The method according to claim 1, further comprising the step of:

logging off the user terminal in response to an encrypted logoff request from the user terminal accompanied by the secure seed.

3. The method according to claim 1, wherein the periodically generating step comprises generating the subsequent session key by concatenating the current session key with the secure seed and applying a hash algorithm.

4. A method for providing a secure communications session with a mobile terminal in a wireless local area network, the method comprising the steps of:

transmitting a secure key and a secure seed to the mobile terminal using a secure communications method, the secure key and the secure seed being suitable for storage in the mobile terminal for use during the secure communications session;

encrypting and transmitting data to the mobile terminal using a current session key, and receiving and decrypting data received from the mobile terminal using the current session key, the secure key initially being used as the current session key; and

periodically generating by an access point a subsequent session key using the secure seed and using the subsequent session key as the current session key during subsequent communications with the mobile terminal.

5. The method as in claim 4, wherein the periodically generating step comprises generating by the access point a subsequent session key using a combination of a new key and the secure seed, the new key being generated using the secure key.

6. The method as in claim 5, wherein the periodically generating step comprises generating by the access point a subsequent session key by concatenating the new key and the secure seed and running a hash algorithm to generate the subsequent session key.

7. A method for providing a secure communications session with a mobile terminal in a wireless local area network, the method comprising the steps of:

generating a secure key;

transmitting the secure key to the mobile terminal using a secure communications method, the secure key being stored in the mobile terminal for use during the secure communications session;

encrypting and transmitting data to the mobile terminal using a current session key, and receiving and decrypting data received from the mobile terminal using the current session key; and

ending the secure communications session by an access point in response to receiving a logoff message from the mobile terminal, the logoff message being in encrypted form and including the secure key.

8. A method for providing a secure communications session with a mobile terminal in a wireless local area network, the method comprising the steps of:

generating a secure key and a secure seed;

transmitting the secure key and the secure seed to the wireless local area network using a secure communications method, the secure key and the secure seed being stored in the wireless local area network for use during the secure communications session;

encrypting and transmitting data to the wireless local area network using a current session key, and receiving and decrypting data received from the wireless local area network using the current session key, the secure key initially being used as the current session key; and

periodically generating by the mobile terminal a subsequent session key using the secure seed and using the subsequent session key as the current session key during subsequent communications with the wireless local area network.

9. The method as in claim 8, wherein the periodically generating step comprises generating by the mobile terminal a subsequent session key using a combination of a new key and the secure seed, the new key being generated using the secure key.

10. The method as in claim 9, wherein the periodically generating step comprises generating by the mobile terminal a subsequent session key by concatenating the new key and the secure seed and running a hash algorithm to generate the subsequent session key.

11. A method for providing a secure communications session with a mobile terminal in a wireless local area network, the method comprising the steps of:

generating a secure key;

receiving the secure key from the wireless local area network using a secure communications method, the secure key being stored in the wireless local area network for use during the secure communications session;

encrypting and transmitting data to the wireless local area network using a current session key, and receiving and decrypting data received from the wireless local area network using the current session key; and

ending the secure communications session in response to receiving a logoff message from the wireless local area network, the logoff message being in encrypted form and including the secure key.

12. A method for providing a secure communications session with a mobile terminal in a wireless local area network, the method comprising the steps of:

installing at least two shared secrets on both the mobile terminal and the wireless local area network access point during the user authentication phase whereby a first secret is the initial session key and a second secret is utilized as secure seed to generate subsequent session keys.

13. The method as in claim 12, further comprising the step of generating a new key and encrypting the new key with the current session key and exchanging and the new key between the wireless local area network and the mobile terminal.

14. The method as in claim 12, further comprising the step of the wireless local area network and the mobile terminal generating a new session key employing the new session key and the secure seed.

15. The method as in claim 14, wherein generating the new session key generation comprises the step of concatenating the said new session key to the secure seed.

16. The method as in claim 15, further comprising the step of generating a new session key by applying a hash algorithm on said concatenated result.

17. The method as in claim 16, further comprising the step of using the said new session key in communications between the wireless local area network and mobile terminal.

18. A method for providing a secure communications session between a mobile terminal and a wireless local area network, the method comprising the steps of:

a mobile terminal sending during session logoff an encrypted logoff request accompanied by the secure seed such that the secure seed appears in the logoff request.

19. An access point for providing a secure communications session between a mobile terminal and a wireless local area network, comprising:

a means for transmitting a secure key and a secure seed to the mobile terminal using a secure communications method;

a means to encrypt data using the secure key; and

a means to periodically generate a subsequent session key using the secure seed.

20. A terminal device for providing a secure communications session with a communications network, comprising:

a means to receive a secure key and a secure seed and a means to store the secure key and the secure seed for use during the secure communications session;

a means to receive data and a means to decrypt the data using a current session key during the secure communications session, the secure key being using initially as the current session key; and

a means to generate a subsequent session key using the current session key and the secure seed, the subsequent session key thereafter being used as the current session key for subsequent communications.

21. The terminal device according to claim 20, wherein the terminal device comprises a mobile terminal and the communications network comprises a wireless local area network.

22. The access point according to claim 24, wherein the means to periodically generate a subsequent session key comprises a means to generate a subsequent session key using a combination of a new key and the secure seed, the new key being generated by means using the secure key.

23. The access point according to claim 24, wherein the means to periodically generate a subsequent session key comprises a means to generate a subsequent session key by concatenating a new key and the second secure seed and a means for running a hash algorithm to generate the subsequent session key.

24. An access point for providing a secure communications session between a mobile terminal and a wireless local area network, comprising:

a means to transmit a secure key and a secure seed and a means to store the secure key and the secure seed for use during the secure communications session;

a means to encrypt data and a means to transmit data to the mobile terminal and a means to receive data and a means to decrypt the data from the mobile terminal using a current session key during the secure communications session, the secure key being using initially as the current session key; and

a means to generate a subsequent session key using the current session key and the secure seed, the subsequent session key thereafter being used as the current session key for subsequent communications.

APPENDIX II. EVIDENCE

None

APPENDIX III. RELATED PROCEEDINGS

The Appellants' previous appeal of 2 December 2008 has been rendered moot by the Examiner's withdrawal of his rejection of 7 August 2008.